UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA

Plaintiff,

Criminal No.: 2:11-cr-470 (SDW)

-vs-

ANDREW AUERNHEIMER,

Defendant.

DEFENDANT'S SENTENCING MEMORANDUM

A. General Sentencing Principles

As a result of *United States v. Booker*, 543 U.S. 220 (2005) and its progeny, including *Gall v. United States*, 552 U.S. 38 (2007), and *Kimbrough v. United States*, 552 U.S. 85 (2007), sentencing courts are permitted to exercise significant discretion in imposing a sentence, and the sentencing options available to district courts have significantly broadened. In making its assessment, a district court is to consider all of the factors in 18 U.S.C. § 3553(a) when tailoring the sentence. While the Federal Sentencing Guidelines are still relevant, they are now only one of seven sentencing factors set forth in § 3553(a) that a district court must consider in determining the applicable sentence. Section 3553(a) provides that a district court should consider:

> The nature and circumstances of the offense and the history and characteristics of the defendant [§3553(a)(1)];
>
> The need for the sentence imposed-

> to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense [§3553(a)(2)(A)];
>
> to afford adequate deterrence to criminal conduct §3553(a)(2)(B)];
>
> to protect the public from further crimes of the defendant [§3553(a)(2)(C)]; and
>
> to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner [§3553(a)(2)(D)];
>
> The kinds of sentences available [§3553(a)(3)];
>
> The kinds of sentence and the sentencing range established in the Federal Sentencing Guidelines [§3553(a)(4)(A-B)];
>
> Any pertinent policy statement issued by the Sentencing Commission [§3553(a)(5)];
>
> The need to avoid unwarranted sentence disparity [§3553(a)(6)]; and
>
> The need to provide restitution to any victims [§3553(a)(7)];

Under *Gall*, district courts must employ a three-step approach when imposing a sentence: (1) determine the applicable Guidelines range; (2) determine if a traditional Guideline departure applies; and (3) determine if a "variance" is appropriate based on consideration of all of the § 3553(a) factors in order to achieve the goal of imposing a sentence that is sufficient but not greater than necessary to accomplish the goals of sentencing. *See Kimbrough*, 552 U.S. at 101.

B. Sentencing Guidelines

According to the Presentence Investigation Report ("PSI") submitted by the United States Probation Office ("Probation"), the defendant has a total Offense Level of 20 and a Criminal History Category of I. According to the current sentencing table, that would result in a Guidelines range of 33 to 41 months imprisonment. However, as discussed below, the defense objects to the PSI's conclusion that the proper Offense Level should be 20.

The defense agrees with the PSI that the base offense level for the crimes for which defendant was convicted is **six**. *See* PSI at ¶ 57; *see also* U.S.S.G. § 2B1.1(a)(2). The defense does not contest that, for the purposes of the Guidelines, the two offenses for which the defendant was convicted involve a continuous course of conduct, and should therefore be grouped together in a single group. *See* PSI at ¶ 56; U.S.S.G. § 3D1.2(d). However, the defense objects to increases based on the purported amount of loss; the double counting for use of a "sophisticated means" and "use of a special skill;" and the enhancement for "dissemination of personal information." *See* PSI at ¶¶ 58 through 67. Therefore, defendant's total offense level under the Sentencing Guidelines should, at most, be a level six, which results in a sentence of no more than zero to six months of imprisonment. The defense suggests a sentence of probation would be appropriate for the reasons that follow.

1. Amount of Loss

According to the PSI, the defendant's offense level should be increased by eight levels because of the loss of $73,167 to AT&T. This assessment is incorrect because: (1) the evidence at trial established no loss to AT&T; (2) the type of loss claimed in the PSI is not the type of loss permitted under the Sentencing Guidelines to enhance a defendant's offense level, because the cost of the breach notification is not directly related to any harm to AT&T's computer servers; and (3) the loss claimed in the PSI was caused primarily by AT&T's duplicative notification to its customers. Increasing the defendant's offense level by eight levels based on this purported loss would result in a manifest injustice.

The evidence at trial established no loss to AT&T. According to the PSI, "AT&T customers suffered no financial losses." PSI at ¶ 53. The PSI states that Probation "provided AT&T with an affidavit form with which to declare any losses and/or submit a statement, [however] no response has been received." *Id.* In fact, when AT&T security personnel first investigated this case, the opinion of at least one AT&T investigator was "I do not believe there is a case here. No security was

circumvented. A poorly crafted/designed feature was available and exploited. We are claiming publicly this poses no threat to customers iPad. I just don't see it." *See* June 10, 2010 email from R. David Hulsey to Marc Kolaks attached hereto as Exhibit A.

Furthermore, under the Sentencing Guidelines and case law, the type of loss claimed in the PSI is not the type of loss which may be attributed to the defendant. The PSI notes a $73,167 "loss" to AT&T based on the alleged cost of a direct mailing to AT&T's iPad subscribers notifying them of the alleged data breach. The direct mailing, however, is not directly related to any harm to AT&T's computer servers, and is therefore not a "loss" under the Computer Fraud and Abuse Act. *See, e.g., Nexans Wires v. Sark USA*, 319 F. Supp. 2d 468, 472-73 (S.D.N.Y. 2004) (costs of travel of senior business executives to meet to discuss response to computer intrusion not a "loss" because it is not sufficiently related to the intrusion); *Int'l Chauffeured Serv. v. Fast Operating Corp.*, 2012 WL 1279825, at *4 (S.D.N.Y. 2012) (holding that the cost of monitoring for indications of further unauthorized access after an initial intrusion was not "loss"); *Shirokov v. Dunlap, Grubb & Weaver*, 2012 WL 1065578, at *24 (D. Mass. 2012) (concluding that legal fees cannot constitute "loss" under the CFAA because they "are not directly attributable to the defendants' alleged access of his computer").

In response to the defendant's objection on this point, the PSI cites to comment n.3(A)(v)(III) of § 2B1.1, which lists a number of items that constitute "actual loss." Each of one these items, however, relates to loss in correcting the damage to computers or servers, and not to incidental or tangential losses. As established by the above-cited cases, costs unrelated to the repair of the computers are not "loss' within the meaning of § 2B1.1

The evidence at trial established, and the PSI acknowledges, that there was no damage to AT&T's computer servers, and no attempt was ever made by either Daniel Spitler or Andrew Auernheimer to alter or damage AT&T's servers.

Moreover, all of the $73,167 "loss" was attributable to AT&T's direct mailing to customers even after it successfully notified its customers by e-mail. AT&T notified its customers of the alleged data breach via e-mail a week before sending out regular mail notifications and the e-mail notifications had a 98.53% success rate. *See* June 15, 2010 email of Nancy Swasey, attached hereto as Exhibit B. Finally, as the testimony at trial established, AT&T did not believe their customers needed to change their email addresses or SIM Cards in response to the incident in question here. *See* Testimony of Sherry Ramsey, Trial Tr. at 39:9-40:3 (Nov. 14, 2012). Therefore, the direct mail notifications to all of AT&T's iPad subscribers were superfluous.

It would be an injustice to raise the defendant's offense level under the Sentencing Guidelines by 8 levels for a tangential cost that was not directly related to a harm to AT&T's computer servers; accordingly, Mr. Auernheimer objects to the eight level increase for loss to AT&T.

2. "Sophisticated Means" and "Use of a Special Skill"

Under the PSI, the defendant's offense level was increased by 2 levels for a purported use of "sophisticated means," and an additional two levels for the purported "use of special skill." *See* PSI at ¶¶ 60 and 65-67. The enhancement of defendant's offense level for both of these elements results in an impermissible double-counting because the two enhancements rely on the identical conduct to justify both enhancements. While both of these enhancements may be used in cases where the two enhancements cover different conduct, the defense objects to the use of the same underlying conduct to raise the Offense Level two levels for use of "Sophisticated Means" and two levels for "Use of a Special Skill" as impermissible double counting.

Moreover, the entirety of § 2.B1.1, and subsection (b)(10) in particular, is directed towards fraudulent behavior. Thus, the level is enhanced only where a defendant uses sophisticated means to perpetuate or conceal a fraud. The PSI does not argue that the defendant used sophisticated means to

perpetuate or conceal a fraud, but only that a sophisticated script was deployed to obtain email addresses.

This reading of "sophisticated means" is consistent with §2.1.1(b)(10), which requires the upward enhancement:

> If (A) the defendant relocated, or participated in relocating, a *fraudulent* scheme to another jurisdiction to evade law enforcement or regulatory officials; (B) a substantial part of a *fraudulent* scheme was committed from outside the United States; or (C) the offense *otherwise* involved sophisticated means. . .
> *Id.* (Emphasis added.)

Thus, as a whole, this provision applies only to fraudulent behavior, as the phrase "otherwise involved" in subsection (C) modifies the previous subsections which involve fraud. Similarly, the examples provided in the Guidelines Manual refer only to fraudulent behavior. § 2.1.1, n(8)(b). Courts have also construed and applied this subsection only where there sophisticated means were used to perpetuate or conceal fraudulent behavior. *See, e.g., United States v. Laguna*, 426 Fed. Appx. 94, 97 (3d Cir. Apr. 28, 2011) (defendant used sophisticated means by setting up fictitious collection agency); *United States v. Sheneman*, 2012 WL 2906859, ** 8-9 (N.D. Ind. July 16, 2012) (enhancement where conduct shows "a greater level of planning or concealment" than a typical fraud of its kind…" (collecting cases)).

3. Dissemination of Personal Information

Under the PSI, defendant's offense level is increased two levels for his purported dissemination of personal information, in the form of "email addresses." PSI at ¶ 61. However, e-mail addresses do not fall under the definition of "personal information" in the Guidelines absent any "sensitive information involving an identifiable individual." The commentary to U.S.S.G. 2B1.1(b)(16) defines "personal information" as "sensitive information involving an identifiable individual…including (A) medical records; (B) wills; (C) diaries; (D) private correspondence,

including e-mail; (E) financial records; (F) photographs of a sensitive or private nature; or (G) similar information."

In a recent decision in the Southern District of New York involving a prosecution under the CFAA, Chief Judge Loretta A. Preska held that there was nothing sensitive about an e-mail address that was obtained by the defendant. *See United States v. Hammond*, 2013 WL 637007 (S.D.N.Y. Feb. 21, 2013). In Hammond, the defendant moved for Judge Preska's recusal, on the basis that one of the e-mail addresses allegedly obtained belonged to the Judge's husband and that others belonged to his clients. Judge Preska denied the motion, reasoning that her husband was not injured by the alleged hack, and that her husband's email address was publicly available on his website. *See id.*, at *7. Moreover, there was no evidence that any of her husband's clients were harmed "beyond the disclosure of certain email addresses, which may or may not have been publicly available previously." *Id.*

The PSI, in its response to the defendant's objections, notes that the definition of "personal identification" is broad enough under the statutes for which the defendant was convicted to include email addresses. Although the defendant does not concede that point, it is irrelevant. The applicable definition of "personal identification" is that under the Guidelines, which is more narrowly tailored and designed only to address identification implicating "sensitive information."

Because only e-mail addresses were involved, with no sensitive information attached, no personal information was disseminated and the increase of two levels is improper.

C. Application of § 3553(a) Factors

After considering the Sentencing Guidelines, the next step for the Court is to determine whether a variance from the Sentencing Guidelines is warranted based on the factors enumerated in § 3553(a). Based on an application of those factors, it is clear that a sentence of probation in the instance case is sufficient but not greater than necessary to accomplish the goals of sentencing.

1. The nature and circumstances of the offense and the history and characteristics of the defendant - §3553(a)(1)

The Court should take into consideration the nature and circumstances of the offense in imposing a sentence. Specifically, the Court should take into consideration the issues raised by the defense in defendant's Motion to Dismiss filed September 21, 2012. Specifically, the defendant did not have "fair notice" that his conduct was illegal, due to the vagueness of the Computer Fraud and Abuse Act (the "CFAA"), 18 U.S.C. § 1030(a)(2)(C). While the issues raised in the motion did not convince the Court to dismiss the Indictment, the Court should consider that other courts and legal scholars have a contrary view, and thus there was no clarity that the conduct attributed to the defendant was illegal. Moreover, in the jurisdiction where the defendant was convicted, there had been no case law interpreting the CFAA, and interpretation of the New Jersey State law which elevates the CFAA charge to a felony was clear that a violation required a circumvention of a password-based restriction or code-based restriction. *See State v. Riley*, 412 N.J. Super. 162, 182 (Sup. Ct. N.J. 2009). The evidence at trial was clear that no password was ever hacked, nor was any attempt ever made to hack a password.

As discussed in defendant's Motion to Dismiss, the CFAA fails to give fair notice in this instance because it nowhere defines what it seeks to make illegal: "intentionally access[ing] a computer without authorization or exceed[ing] authorized access . . . ." *See* 18 U.S.C. § 1030(a)(2). This lack of clarity has caused understandable consternation among the federal courts as they attempt to divine the meaning of what Congress has declined to define. *See United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009) (holding the CFAA constitutionally void for vagueness as

applied); *Shamrock Foods Co. v. Gast*, 535 F.Supp. 2d 962, 964-65 (D. Ariz. 2008) (discussing the conflicting approaches to unauthorized access among the federal courts in civil cases); Andrew T. Hernacki, A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act, 61 Am. U. L. Rev. 1543, 1554 (2012) ("[C]ourts and academics have struggled to interpret these undefined and vague provisions . . . ."); Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L. Rev. 1561, 1572 (2010) ("Exactly what is an 'access,' and what makes an 'access' unauthorized, is presently unclear."). To severely punish a defendant on the basis of a law that lacks clarity is unjust.

2. The need for the sentence imposed: to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense [§3553(a)(2)(A)]; to afford adequate deterrence to criminal conduct §3553(a)(2)(B)]; to protect the public from further crimes of the defendant [§3553(a)(2)(C)]; and to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner [§3553(a)(2)(D)];

A sentence of probation in this matter would be adequate to reflect the seriousness of the offense, to afford adequate deterrence, and to protect the public from further crimes. Prior to this incident, the defendant had no criminal convictions, and since being arrested he has full complied with the conditions of his bail.

3. The need to avoid unwarranted sentence disparity [§3553(a)(6)]

The need to avoid unwarranted sentence disparity is an important issue that should be considered by the Court. In a recent CFAA prosecution alleging far more intrusive facts, the Department of Justice is on record that no more than six months of imprisonment was appropriate.

On March 6, 2013, Attorney General Eric H. Holder, Jr. testified before the Senate Committee on the Judiciary regarding the case of Aaron Swartz. Mr. Swartz was indicted for, among other things, wire fraud, computer fraud, and unlawfully obtaining information from a protected computer. *See United States v. Aaron Swartz*, Superseding Indictment, 11-CR-10260

(NMG) (D.Mass. Sept. 12, 2012). Mr. Swartz committed suicide on January 11, 2013 before his trial. In response to questions regarding the Department of Justice's handling of the Mr. Swartz's case, Attorney General Holder stated:

> An offer – a plea offer – was made to him of 3 months before the indictment; this case could've been resolved in a plea of 3 months. After the indictment, an offer was made he could plea and serve 4 months, even after that a plea offer was made in a range 0 – 6 months that he would be able to argue for a probationary sentence, the government would be able to argue for up to a period 6 months, there was never an intention for him to go to jail for longer than a 3, 4, potentially 5 month range – that was what the government said specifically to Mr. Swartz, those offers were rejected.
> *See*
> http://www.judiciary.senate.gov/hearings/hearing.cfm?id=e0c4315749c10b084028087a4aa80a73

Therefore, it is the position of the Department of Justice that conduct arguably more egregious than the defendant's conduct in the instant case merits a term of imprisonment in the 0 to 6 month range. Thus, a 33 to 41 month range recommended in the PSI does not accord with the the Department of Justice's view of an appropriate sentence for a CFAA violation allegedly involving more egregious acts than those in question here.

D. The Purpose of Sentencing

Section 3553(a)(2), discussed above, identifies the goals of sentencing, which are: (1) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (2) to afford adequate deterrence to criminal conduct; (3) to protect the public from further crimes of the defendant; and (4) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner. The Defendant has complied with all the terms of his pre-trial bail conditions. The sentence which the Defense suggests to the Court, a term of noncustodial probation, would be adequate but no greater than necessary to accomplish the purposes of sentencing.

CONCLUSION

The Court is to "consider every convicted person as an individual and every case as a unique study in the human failings that sometimes mitigate, sometimes magnify, the crime and the punishment to ensue." *Gall* at 52 (quoting *Koon v. United States*, 518 U.S. 81, 98 (1996)). The ultimate goal, as described above, is to impose a sentence that is sufficient, but not more than necessary, to accomplish the goals of sentencing. Mr. Auernheimer respectfully submits that a sentence of noncustodial probation would do just that.

Respectfully submitted,

Tor Ekeland
Mark H. Jaffe
Tor Ekeland, PC
155 Water Street
Brooklyn, NY 11201
718 285 9343
718 504 5417 fax
tor@torekeland.com

Nace Naumowski
Paris Ackerman & Schmierer LLP
618 Newark Avenue
Elizabeth, NJ 07208
908 349 8462
908 325 1646 fax
nace@paslawfirm.com

CERTIFICATION OF SERVICE

I, Tor Ekeland, hereby declare under the penalty of perjury that on March 13, 2012, I sent true copies of the foregoing via email to the Honorable Susan D. Wigenton, and Executive Assistant United States Attorney Michael Martinez and Assistant United States Attorney Zach Intrater.

I certify that the foregoing statements made by me are true. I am aware that if any of the foregoing statements made by me are willfully false, I am subject to punishment for contempt.

Tor Ekeland

Dated: March 13, 2012

Tor Ekeland

EXHIBIT A

From: HULSEY, R DAVID (ATTSI)
To: KOLAKS, MARC S (ATTSI)
Sent: 6/10/2010 3:07:50 PM
Subject: Re: FBI Interest in iPad issue

ATT 002102

EXHIBIT B

From: SWASEY, NANCY J (ATTOPS)
To: IZBRAND, JOE (ATTSI); WOLFE, ANNE (ATTSI); RAMSEY, SHERRY L (ATTSI); OSMOND, KATHLEEN (ATTOPS); HULSEY, R DAVID (ATTSI); 'Hausken, Eric'; EUBANK, KIMBERLY D (ATTCINW); PEGUES, SUNSHINE (ATTCINW); ISOM, ANNETTE H (ATTOPS); GALBRAITH, TINA A (Legal); PARRA-GAONA, MARISIA (Legal); EPSTEIN, KEITH J (Legal); TYPROWICZ, TODD J (ATTOPS); HARGREAVES, MARK (ATTSI); TOCCO, JOSEPH (Legal)
Sent: 6/15/2010 1:50:51 AM
Subject: Early E-mail Bounceback Report

ATT 002751